dr inż. Dominika Lisiak-Felicka
Uniwersytet Łódzki
dr Maciej Szmit
Orange Labs Poland

WYBRANE ASPEKTY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W URZĘDACH MARSZAŁKOWSKICH

Wprowadzenie

Przez „System Zarządzania Bezpieczeństwem Informacji" (SZBI, ang. Information Security Management System) rozumie się (według definicji zawartych w normach ISO/IEC z serii 27000), część systemu zarządzania, opierającą się na koncepcji zarządzania ryzykiem biznesowym, a odpowiedzialną za ustanowienie, wdrożenie, funkcjonowanie, monitorowanie, przeglądy, utrzymanie i doskonalenie bezpieczeństwa informacji, przy czym sam system zarządzania jest rozumiany jako zbiór wytycznych, polityk, procedur, procesów i związanych z nimi zasobów (a więc zarówno zasobów materialnych, takich jak komputery czy maszyny, zasobów ludzkich – jak pracownicy wraz z ich umiejętnościami i doświadczeniem, jak i zasobów niematerialnych – jak programy komputerowe czy kultura organizacyjna) mających na celu zapewnienie organizacji spełnienia swoich zadań (por. ISO/IEC 27000:2009, Gillies, 2011, s. 367-376, Humphreys, 2007, s. 11-44).

Na podkreślenie zasługują przynajmniej dwa elementy definicji normatywnych:

- podejście systemowe, w szczególności związane z tym, że SZBI tworzą nie tylko same „papierowe" zapisy (procedury, normy, zarządzenia itd.) ale i wszelkie zasoby mające związek z bezpieczeństwem informacji oraz
- oparcie bezpieczeństwa informacji na koncepcji zarządzania ryzykiem biznesowym (por. PN-ISO 31000:2012). Zgodnie z tym podejściem, elementami zarządzania ryzkiem (rozumianym w ogólności jako skutek niepewności, a w szcze-

ISSN: 1898-4509

gólności – w odniesieniu do ryzyka zagrożeń – jako kombinacja prawdopodobieństwa zmaterializowania się potencjalnego zagrożenia i jego skutków, a więc jako wartość oczekiwana potencjalnych strat wynikających ze zrealizowania się potencjalnego zagrożenia) jest jego oszacowanie oraz zaplanowanie odpowiedniego postępowania z nim (a więc podjęcie decyzji o jego uniknięciu, akceptacji, przeniesieniu itp.), przy czym oczywiście podejście biznesowe prowadzi do wniosku, że wartość środków poniesionych na wybrany sposób postąpienia z danym ryzykiem nie może przekraczać spodziewanej wartości strat wynikłych z konsekwencji ewentualnego zmaterializowania się zagrożeń (por. np. Staniec, Zawiła-Niedźwiecki, 2008, s. 201-228).

Ten ostatni element może budzić wątpliwość w odniesieniu do zarządzania bezpieczeństwem informacji w organizacjach niebiznesowych, w tym w urzędach administracji państwowej i samorządowej. O ile bowiem dla organizacji gospodarczej stosunkowo łatwo (przynajmniej co do zasady) jest oszacować ekonomiczną wartość naruszenia bezpieczeństwa poszczególnych informacji (zob. np. McCandless, World's Biggest Data Breaches & Hacks, Białas, 2007), o tyle administracja państwowa, rządowa czy samorządowa nie kieruje się zasadą maksymalizacji zysku. Jednostki samorządu terytorialnego (w kontekście prowadzonego badania – samorządy województw, których zarządy wykonują zadania przy pomocy urzędów marszałkowskich), finansowane są z budżetu państwa (w postaci dotacji celowej i subwencji ogólnej) oraz z dochodów własnych (Ustawa z dnia 13 listopada 2003 r., Jastrzębska, 2012, s. 106-130), przy czym dochody własne stanowią zdecydowanie mniejszą część wpływów. Dlatego też kategoria ryzyka biznesowego, w przypadku tych jednostek, może nie być najlepszą dla szacowania potencjalnych skutków naruszenia bezpieczeństwa, niemniej jednak podejście opisane w normach z serii ISO/IEC 27k stosuje się również (zresztą zgodnie z określonym w nich zakresem) we wszystkich typach organizacji, a więc w szczególności również, w urzędach.

Zagadnienie zarządzania bezpieczeństwem informacji w urzędach jest interesujące z szeregu powodów:

- bezpieczeństwo informacyjne urzędów ma bezpośredni związek z bezpieczeństwem obywateli. O ile każdy samodzielnie decyduje czy zostać użytkownikiem takiego czy innego systemu informatycznego, czy powierzyć swoje dane komercyjnej firmie, w jaki sposób je przechowywać czy przetwarzać, o tyle kontakt obywateli z urzędami i przetwarzanie przez nie ich danych są obowiązkowe z mocy prawa.

- Urzędy mają ściśle zdefiniowany zakres swoich zadań i kompetencji, stosunkowo łatwe jest więc przeprowadzenie analizy porównawczej dotyczącej zarządzania bezpieczeństwem informacji w różnych urzędach, rola bowiem „specyfiki przedsiębiorstwa" tak ważna w organizacjach komercyjnych jest w przypadku urzędów minimalna (Calder, 2005, s. 107-112, Kister, 2009, s. 329-334, Robinson, 2005, s. 45-49).
- Urzędy, z uwagi na zasadę jawności i możliwość dostępu do informacji publicznej stanowią szczególnie wygodny materiał badawczy, i choć praktyka pokazuje, że tendencja do ukrywania informacji jest wśród pracowników urzędów obecna, to jednak responsywność badań jednostek organizacyjnych administracji publicznej jest zdecydowanie wyższa niż w przypadku organizacji komercyjnych.

1. Cel i metoda badania

Zarządzanie bezpieczeństwem informacji (Ilvonen, 2011, s. 148-154, Jašek, 2005, s. 45-48, Korzeniowski, 2005, s. 20-23, Stoll, Breu, 2013, s. 11-23) jest wielkim wyzwaniem dla współczesnych organizacji i instytucji. Urzędy administracji państwowej, rządowej i samorządowej nie stanowią w tym względzie wyjątku, wystarczy wspomnieć o licznych wyciekach informacji, i włamaniach do różnych organizacji państwowych, opisywanych w popularnej prasie (o czym świadczą – przykładowo – choćby takie tytuły: *Włamanie hakera na stronę internetową Inowrocławia*, *Urzędy gmin są bezradne wobec hakerów*, *Ktoś włamał się na serwer ratusza. Dzwonił do Zimbabwe*, *Poszukiwania hakera, który włamał się na stronę płockiego UM*), stąd też celowym wydawało się przeprowadzenie badania dotyczącego rozwiązań przyjętych w wybranych urzędach. Urzędy marszałkowskie wydawały się dobrym przedmiotem badania, zarówno z uwagi na ich liczbę (a więc, co za tym idzie – ograniczony koszt takiego badania), jak i charakter (z jednej strony są to urzędy na tyle duże, że różne aspekty zarządzania nimi powinny być prowadzone zgodnie ze sformalizowanymi metodykami, z drugiej – urzędy takie nie mają do czynienia z informacją zastrzeżoną – np. z tajemnicami państwowymi, co utrudniłoby badanie).

Badanie miało przede wszystkim cel poznawczy, to jest odpowiedź na pytania: w których urzędach marszałkowskich wdrożone są systemy zarządzania bezpieczeństwem informacji, jak wyglądało ich wdrożenie i funkcjonowanie oraz jak wygląda w tych urzędach praktyka zarządzania incydentami bezpieczeństwa informacji.

W ramach prac badawczych przeprowadzono badanie ankietowe z wykorzystaniem kwestionariusza ankietowego umieszczonego w Internecie.

2. Wyniki badania

Kwestionariusz ankietowy wypełnili przedstawiciele 13 urzędów. Urząd Marszałkowski Województwa Podlaskiego przesłał pisemną informację o braku zainteresowania udziałem w badaniu ankietowym, natomiast dwa urzędy (Urząd Marszałkowski Województwa Dolnośląskiego i Urząd Marszałkowski Województwa Kujawsko-Pomorskiego), pomimo licznych kontaktów telefonicznych i mailowych ze strony ankietującego, nie przesłały żadnych odpowiedzi.

Wśród 13 urzędów marszałkowskich, w 9 jest wdrożony system zarządzania bezpieczeństwem informacji. W 4 urzędach (województwa: lubelskie, łódzkie, śląskie, świętokrzyskie), taki system nie funkcjonuje i w przeszłości nie były podejmowane próby jego wdrożenia. Jedynie w trzech urzędach marszałkowskich (województwa: lubuskie, małopolskie, mazowieckie) podjęto decyzję o certyfikacji systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001.

Spośród 13 badanych urzędów, 12 ma opracowaną i wdrożoną politykę bezpieczeństwa informacji zawierającą politykę ochrony danych osobowych zgodną z wymaganiami ustawy o ochronie danych osobowych (Ustawa z dnia 5 czerwca 1998 r., Monarcha-Matlak, 2008, s. 239-268, Suchorzewska, 2010, s. 279-285), a jeden z urzędów (Urząd Marszałkowski Województwa Podkarpackiego) posiada tylko politykę ochrony danych osobowych zgodną z wymaganiami ustawy o ochronie danych osobowych (Ustawa z dnia 29 sierpnia 1997 r.).

Szczegółowe wyniki części badania dotyczącej wdrożenia i funkcjonowania SZBI opublikowano i omówiono w artykule (Lisiak-Felicka, Szmit, 2013). Poniżej prezentujemy wyniki dotyczące praktyki zarządzania incydentami bezpieczeństwa.

Spośród 13 badanych urzędów marszałkowskich jedynie 7 podało informację, że incydenty bezpieczeństwa (Maj, Silicki, 2013, Ludwiszewski, 2009, s. 123-142) zdarzały się i były rejestrowane.

Liczby incydentów oraz opis sposobu zarządzania nimi w poszczególnych urzędach zostały przedstawione w tabeli 1 i tabeli 2.

Tab. 1. Liczba incydentów bezpieczeństwa w urzędach marszałkowskich

Lp.	Województwo	2010	2011	2012
1.	małopolskie	20	15	7
2.	mazowieckie	9	5	6
3.	pomorskie	1	1	0
4.	śląskie	3	2	4
5.	warmińsko-mazurskie	1	0	0
6.	wielkopolskie	brak rejestru	kilka	6
7.	zachodniopomorskie	Urząd nie chce ujawnić informacji		

Źródło: opracowanie własne.

Tab. 2. Sposoby zarządzania incydentami w urzędach marszałkowskich

Lp.	Województwo	Opis sposobu zarządzania incydentami bezpieczeństwa
1.	małopolskie	Dokonuje się kwartalnego przeglądu zaistniałych incydentów naruszenia bezpieczeństwa informacji. W odniesieniu do każdego incydentu podejmuje się działania korygujące i naprawcze.
2.	mazowieckie	Wszystkie kwestie związane z zarządzaniem incydentami zostały opisane w procesie zintegrowanego systemu zarządzania.
3.	pomorskie	Analiza incydentu, rozliczenie osób odpowiedzialnych, wdrożenie procedur PBI
4.	śląskie	1. Stwierdzenie/zgłoszenie incydentu. 2. Podjęcie działań proceduralnych przez osoby odpowiedzialne za wymagane decyzje oraz osoby odpowiedzialne za wykonanie czynności technicznych. 3. Przeprowadzanie działań naprawczo-korygujących oraz jeśli jest to wymagane, jednoczesne udokumentowanie opisu zdarzenia i podjętych działań. 4. Omówienie incydentu i w razie potrzeby sformułowanie wniosków z proponowanymi modyfikacjami lub nowymi rozwiązaniami do wdrożenia.
5.	warmińsko-mazurskie	1. Ustalenie charakteru incydentu 2. Jak najszybsze działanie w celu minimalizacji skutków 3. Zgłoszenie do odpowiednich organów
6.	wielkopolskie	Zgłaszanie incydentów odbywa się do helpdesku i do ABI gdzie są rejestrowane. W przypadkach gdy helpdesk stwierdzi naruszenie PBI zgłaszane jest to do ABI. Następnie na spotkaniach Zespołu incydenty są omawiane oraz podejmowana jest decyzja o wdrożeniu niezbędnych rozwiązań organizacyjnych czy technicznych.
7.	zachodniopomorskie	Identyfikacja incydentu - wszczęcie postępowania wyjaśniającego - prowadzenie czynności wyjaśniających - określenie potrzeby poinformowania właściwych służb - podjęcie działań naprawczych i zapobiegawczych (wdrożenie) - kontrola - zamknięcie postępowania

Źródło: opracowanie własne.

Jedynie w przypadku Urzędu Marszałkowskiego Województwa Mazowieckiego i Urzędu Marszałkowskiego Województwa Warmińsko-Mazurskiego incydenty bezpieczeństwa były zgłaszane policji. Urząd Marszałkowski Województwa Wielkopolskiego zgłosił do tej pory jeden incydent do tej instytucji, wyjaśnił również, że „nie wszystkie incydenty kwalifikowały się do zgłoszenia do cert.gov.pl czy też prokuratury. Procedury obejmują postępowanie, że w przypadku kradzieży urządzeń ma być to zgłoszone policji.

Cert.gov.pl zgłosiło również do nas szereg błędów które zostały zminimalizowane przez zastosowanie dodatkowych rozwiązań zabezpieczających przed zagrożeniami z Internetu".

Tylko Urząd Marszałkowski Województwa Pomorskiego wskazał, że może liczyć na wsparcie ze strony innych organów administracji w zakresie zarządzania incydentami. Określił to wsparcie jako „pomoc merytoryczną".

Urzędnicy zostali poproszeni o wskazanie fizycznych zabezpieczeń dostępu do informacji. Odpowiedzi zostały przedstawione na rysunku 1.

Rys. 1. Fizyczne zabezpieczenia dostępu do informacji

Źródło: opracowanie własne.

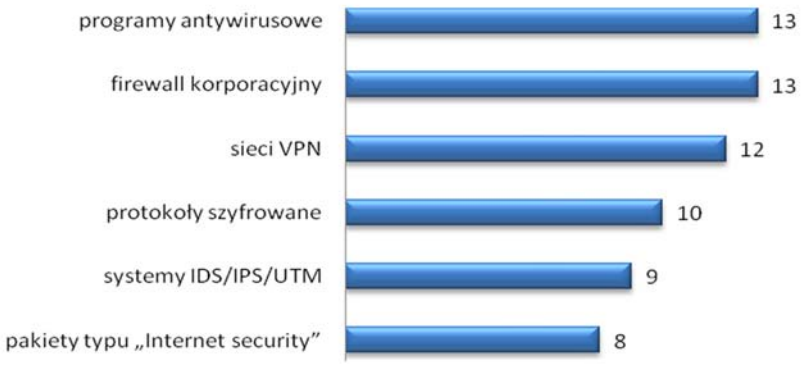
Urzędnicy wskazali również dodatkowe, stosowane w ich urzędach zabezpieczenia:

- agencja ochrony, służby ochrony obiektów,
- system kontroli dostępu do pomieszczeń,
- plombowane wejścia do pomieszczeń.

Wśród wdrożonych zabezpieczeń systemów informatycznych najbardziej popularne są programy antywirusowe i firewalle korporacyjne.

Szczegółowe zestawienie wskazanych przez urzędników zabezpieczeń zostało przedstawione na rysunku 2.

Rys. 2. Zabezpieczenia systemów informatycznych w urzędach marszałkowskich



Źródło: opracowanie własne.

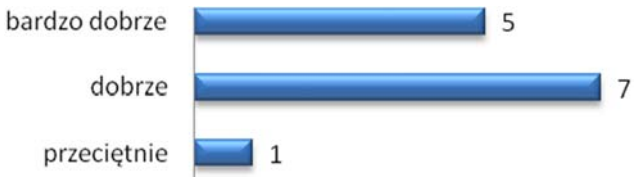
Dodatkowe zabezpieczenia wymieniane przez urzędników to miedzy innymi:

- Systemy Check Point,
- segmentacja fizyczna i logiczna LAN, UPS, generator prądu, redundancja połączeń i zasilania oraz urządzeń.

We wszystkich badanych urzędach prowadzone są szkolenia z zakresu bezpieczeństwa informacji, bezpieczeństwa systemów informatycznych, ochrony danych osobowych.

Na rysunku 3 przedstawiono oceny poziomów bezpieczeństwa informacji w urzędach dokonane przez urzędników.

Rys. 3. Oceny poziomów bezpieczeństwa informacji w urzędach marszałkowskich



Źródło: opracowanie własne.

Liczby szkoleń oraz liczby osób biorących udział w tych szkoleniach w roku 2011 zostały przedstawione w tabeli 3.

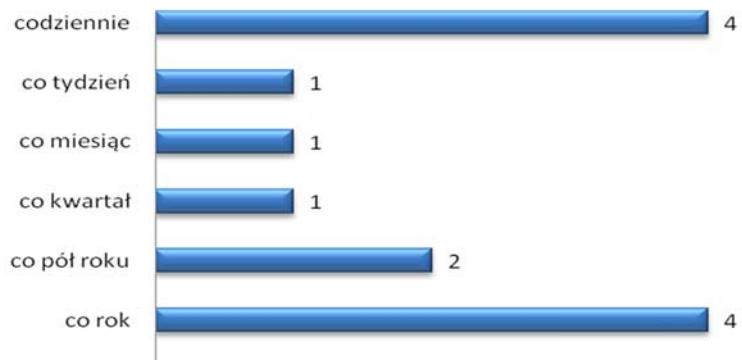
Tab. 3. Liczby szkoleń oraz liczby uczestników w roku 2011

Lp.	Województwo	Liczba szkoleń w 2011 r.	Liczba uczestników szkoleń w 2011 r.
1.	lubelskie	2	2
2.	lubuskie	1	600
3.	łódzkie	10	ponad 100
4.	małopolskie	5	200
5.	mazowieckie	10	300
6.	opolskie	8	135
7.	podkarpackie	około 100	około 350
8.	pomorskie	10	1000
9.	śląskie	około 30	około 300
10.	świętokrzyskie	2	około 415
11.	warmińsko-mazurskie	5	57
12.	wielkopolskie	16	234
13.	zachodniopomorskie	12	około 200

Źródło: opracowanie własne.

Interesujące w kontekście tematyki niniejszego artykułu są również odpowiedzi na pytanie o częstotliwość przeglądów bezpieczeństwa (rys. 4).

Rys. 4. Częstotliwość prowadzenia przeglądów bezpieczeństwa



Źródło: opracowanie własne.

W ramach badania sprawdzono również, jakie inne systemy (Batko, 2009, s. 93-156) zostały wdrożone w badanych urzędach. Wyniki zostały przedstawione w tabeli 4.

Tab. 4. Inne systemy wdrożone w urzędach marszałkowskich

Lp.	Województwo	Systemy wskazane w kwestionariuszu	Inne, wskazane przez urzędników
1.	lubelskie	System Zarządzania Jakością (ISO 9001)	-
2.	lubuskie	System Zarządzania Jakością (ISO 9001)	-
3.	łódzkie	System Zarządzania Jakością (ISO 9001)	System Przeciwdziałania Zagrożeniom Korupcyjnym SPZK
4.	małopolskie	System Zarządzania Jakością (ISO 9001)	Zintegrowany System Zarządzania został rozbudowany o kolejne dwa elementy: System Zarządzania Bezpieczeństwem i Higieną Pracy oraz System Bezpieczeństwa Informacji. Kolejnym krokiem do rozwoju i doskonalenia Zintegrowanego Systemu Zarządzania było wdrożenie wymagań dodatkowych Systemu Przeciwdziałania Zagrożeniom Korupcyjnym oraz ich integracja z funkcjonującym w Urzędzie ZSZ.
5.	mazowieckie	System Zarządzania Jakością (ISO 9001)	ISO 9001 (PN-EN ISO 9001:2009), ISO 14000 (ISO 14001:2004), OHSAS 18000 (OHSAS 18001:1999)0, System Przeciwdziałania Zagrożeniom Korupcyjnym 2010
6.	opolskie	System Zarządzania Jakością (ISO 9001)	-
7.	podkarpackie	-	System bezpieczeństwa informacji niejawnych i innych tajemnic prawnie chronionych System ochrony danych osobowych Systemy zarządzania ciągłością działania
8.	pomorskie	-	-
9.	śląskie	System Zarządzania Jakością (ISO 9001)	-
10.	świętokrzyskie	-	-
11.	warmińsko-mazurskie	System Zarządzania Jakością (ISO 9001)	-
12.	wielkopolskie	-	-
13.	zachodniopomorskie	System Zarządzania Jakością (ISO 9001)	-

Źródło: opracowanie własne.

Wnioski

Wyniki badania potwierdzają, że zagadnienia związane z bezpieczeństwem informacji są znane urzędnikom, zwłaszcza w zakresie ochrony danych osobowych. Wszystkie badane urzędy posiadają stosowną dokumentację, w każdej jednostce powołano administratora bezpieczeństwa informacji, wszystkie jednostki posiadają odpowiednie zabezpieczenia fizycznego dostępu do informacji i stosowne zabezpieczenia systemów informatycznych. Urzędnicy realizują zatem zadania wynikające z przepisów dotyczących ochrony danych osobowych (Rozporządzenie MSWiA z dnia 29 kwietnia z 2004 r., Ustawa z dnia 29 sierpnia 1997 r.).

W 9 urzędach, z 13 biorących udział w badaniu zadeklarowano wdrożenie SZBI, jednak informacje dotyczące częstotliwości przeglądu SZBI oraz liczby odnotowanych incydentów i sposobu reakcji na nie muszą budzić wątpliwości odnośnie do jakości niektórych wdrożeń. Przegląd jest czynnością podjętą w celu określenia przydatności, adekwatności i skuteczności przedmiotu (w tym przypadku: SZBI) w celu osiągnięcia założonych celów (patrz: 3.8.2.2 w ISO Guide 73 Risk management, 2009). Przeglądy mogą być przeprowadzane co kilka miesięcy lub w przypadku konieczności, ale nie jest ani możliwe, ani celowe dokonanie przeglądu SZBI (którego dokumentacja w poszczególnych urzędach ma przecież, jak wynika z badania co najmniej kilkadziesiąt stron) co tydzień lub nawet codziennie. Tymczasem niemal połowa respondentów taką właśnie częstotliwość podała. Dziwi również liczba incydentów bezpieczeństwa informacji.

Urzędy marszałkowskie zatrudniają po kilkaset osób, z czego większość ma do czynienia z narzędziami komputerowymi, wydaje się więc niezwykle mało prawdopodobne, żeby nie zdarzały się incydenty bezpieczeństwa przynajmniej takie jak zgubienie/kradzież urządzeń mobilnych, infekcja złośliwym oprogramowaniem, ujawnienie haseł, problemy z kopiami bezpieczeństwa itd., nie mówiąc już o incydentach poważniejszych. Mała liczba zgłoszeń incydentów może świadczyć o zgłaszaniu tylko najpoważniejszych z nich. Braku zgłoszenia wykrytego incydentu nie stanowi sam w sobie dużego zagrożenia (o ile oczywiście zostały podjęte odpowiednie działania korygujące i naprawcze), choć z drugiej strony utrudnia powołanym do tego instytucjom jak rządowy zespół CERT (cert.gov.pl) choćby statystyczną analizę częstości tego rodzaju zdarzeń.

Nie tylko administracja samorządowa zgłasza małą liczbę incydentów. Taka sytuacja dotyczy całej administracji publicznej w Polsce (państwowej, rządowej i samorządowej). Jak pokazują wyniki raportów Rządowego Zespołu Reagowania na Incydenty Komputerowe (cert.gov.pl) (Raport o stanie bezpieczeństwa cyberprzestrzeni RP, 2011, 2012,

2013), w 2010 zespół ten odnotował 621 zgłoszeń, z czego 155 zostało zakwalifikowanych jako faktyczne incydenty. W roku 2011 zarejestrowano 854 zgłoszenia, z których 249 zakwalifikowano jako faktyczne incydenty. Natomiast w 2012 r. zarejestrowano 1168 zgłoszeń, z których 457 zostało zakwalifikowanych jako faktyczne incydenty.

Jako pozytywne można uznać jedynie fakty, że liczby zgłaszanych incydentów wykazują tendencję wzrostową oraz zwiększa się udział faktycznych incydentów w ogólnej liczbie zgłoszeń. Można spodziewać się, że liczby zgłaszanych incydentów w przyszłości będą rosły, gdyż zgodnie z przyjętą przez Radę Ministrów Polityką Ochrony Cyberprzestrzeni RP (Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, 2013), ocena skuteczności jej wprowadzenia ma się odbywać poprzez podane przykładowe mierniki produktu (polityki), którymi są: liczba odpowiedzi na zgłoszone incydenty oraz liczba obsłużonych incydentów.

Niezwykle ważną kwestię stanowią szkolenia z zakresu bezpieczeństwa informacji, bezpieczeństwa systemów informatycznych, czy ochrony danych osobowych. Wyniki badania wskazują, że urzędnicy we wszystkich 13 urzędach marszałkowskich mają możliwość uczestniczenia w takich formach kształcenia, jakkolwiek liczby szkoleń w poszczególnych jednostkach są bardzo różne (od 2 do około 100). Wynik Urzędu Marszałkowskiego Województwa Podkarpackiego wydaje się być zaskakująco dobry, przy ogólnej tendencji administracji samorządowej do minimalizowania wydatków budżetowych, w tym wydatków na szkolenia pracowników.

Literatura

Batko J. (2009), *Zarządzanie jakością w urzędach gminy*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków

Białas A. (2007), *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwo WNT, Warszawa

Calder A. (2005), *Nine Steps to Success: an ISO 27001 Implementation Overview*, IT Governance Publishing

European Network Security Institute Sp. z o.o., *Dokumentacja metodyki TISM*, http://www.ensi.net/ [15.10.2013]

Gillies A. (2011), *Improving the quality of information security management systems with ISO27000*, "TQM Journal", Vol. 23, Iss. 4

Humphreys E. (2007), *Implementing the ISO/IEC 27001 Information Security Management System Standard*, Artech House, Norwood

Ilvonen I. (2011), *Information security culture or information safety culture – What do words convey?*, 10th European Conference on Information Warfare and Security 2011, ECIW, Tallinn

ISO 14001:2004 – Systemy Zarządzania Środowiskowego – Wymagania i wytyczne stosowania

ISO Guide 73 Risk management – Vocabulary. First edition, ISO 2009

ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems – Overview and vocabulary

Jašek R. (2005), *The information security of enterprises and citizens' security context*, "Komunikacie", Vol. 7, Iss. 3

Jastrzębska M. (2012), *Finanse jednostek samorządu terytorialnego*, Wolters Kluwer Polska

Kister Ł. (2009), *Significance of information security in a company*, (w:) *Riešenie krízových situácií v špecifickom prostredí*, Žilinska univerzita, Žilina

Korzeniowski L. (2005), *Securitology – The concept of safety*, "Komunikacie", Vol. 7, Issue 3

Ktoś włamał się na serwer ratusza. Dzwonił do Zimbabwe, http://lublin.gazeta.pl/lublin/1,35640,8213185,Ktos_wlamal_sie_na_serwer_ratusza__Dzwonil_do_Zimbabwe.html [15.10.2013]

Lisiak-Felicka D., Szmit M. (2013), *Information Security Management Systems in Marshal Offices in Poland*, paper notified at the VIII Scientific Conference „Information Systems In Management", taking place on 21-22 November 2013

Ludwiszewski M. (2009), *Monitoring stanu bezpieczeństwa teleinformatycznego państwa* (w:) Madej M. (red.): *Bezpieczeństwo Teleinformatyczne Państwa*, Polski Instytut Spraw Międzynarodowych

Maj M., Silicki K. (2013), *Klasyfikacja i terminologia incydentów naruszających bezpieczeństwo sieci*, CERT POLSKA, Łódź http://www.cert.pl/PDF/SECURE99_referatCP_klasyf.doc [15.10.2013]

McCandless D., *World's Biggest Data Breaches & Hacks* http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ [15.10.2013]

Monarcha-Matlak A. (2008), *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer Polska

OHSAS 18001:1999 Occupational health and safety management systems – Specification

PN-EN ISO 9001:2009 – Systemy zarządzania jakością – Wymagania

PN-ISO 31000:2012 – Zarządzanie ryzykiem – Zasady i wytyczne

PN-ISO/IEC 17799:2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej (2013), Ministerstwo Administracji i Cyfryzacji, Warszawa

Poszukiwania hakera, który włamał się na stronę płockiego UM http://www.zw.com.pl/artykul/605710.html [15.10.2013]

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2010 r. (2011), Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), Warszawa, http://www.cert.gov.pl/portal/cer/57/422/Raport_o_stanie_bezpieczenstwa_cyberprzestrzeni_RP_w_2010_roku.html [15.10.2013]

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2011 r. (2012), Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), Warszawa, http://www.cert.gov.pl/portal/cer/57/549/Raport_o_stanie_bezpieczenstwa_cyberprzestrzeni_RP_w_2011_roku.html [15.10.2013]

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2012 r. (2013), Rządowy Zespół Reagowania Na Incydenty Komputerowe (cert.gov.pl), Warszawa, http://www.cert.gov.pl/portal/cer/57/605/Raport_o_stanie_bezpieczenstwa_cyberprzestrzeni_RP_w_2012_roku.html [15.10.2013]

Robinson N. (2005), *IT excellence starts with governance*, "Journal of Investment Compliance", Vol. 6, Iss. 3

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia z 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz.U. nr 100 poz. 1024)

Staniec I., Zawiła-Niedźwiecki J. (2008), *Zarządzanie ryzykiem operacyjnym*, Wydawnictwo C.H. Beck, Warszawa

Stoll M. , Breu R. (2013), *Information security measurement roles and responsibilities*, 6th International Joint Conference on Computer, Information and Systems Sciences and Engineering, "Lecture Notes in Electrical Engineering"

Suchorzewska A. (2010), *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer Polska

Urzędy gmin są bezradne wobec hakerów, http://blog.rp.pl/goracytemat/2011/09/27/urzedy-gmin-sa-bezradne-wobec-hakerow/ [15.10.2013]

Ustawa z dnia 13 listopada 2003 r. *o dochodach jednostek samorządu terytorialnego* (Dz.U. 2003 nr 203 poz. 1966 z późn. zm.)

Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. z 1997, Nr 133, poz. 883, z późn. zm.)

Ustawa z dnia 5 czerwca 1998 r. *o samorządzie województwa* (Dz. U. z 2001 r. Nr 142, poz. 1590 z późn. zm.)

Włamanie hakera na stronę internetową Inowrocławia, http://www.pomorska.pl/apps/pbcs.dll/article?AID=/20090216/INOWROCLAW01/825082506 [15.10.2013]

* * *

Artykuł uzyskał pozytywne opinie wydane przez dwóch niezależnych Recenzentów.

Dominika Lisiak-Felicka
Maciej Szmit

Selected apects of information security management in marshal office

Abstract

The article presents results of a survey concerning Information Security Management Systems (ISMS), which was conducted in Marshal Offices between December 2012 and April 2013. The aim of the research was identifying in which government offices ISMS are implemented, according to which standards are developed and certified and gathering information about documentation concerning information security.

The article is an extended version of the paper notified at the VIII Scientific Conference „Information Systems In Management", taking place on 21-22 November 2013.

Key words: information security, information security management systems, information security policy

Резюме

В статье представлены результаты опроса по Системам Управления Информационной Безопасностью (СУИБ), проведенного в государственных учреждениях Польши за период 12.2012-04.2013. Целью опроса было определить, в которых государственных учреждениях внедрены СУИБ, а также собрать информацию о документации по информационной безопасности.

Статья представляет собой расширенный вариант доклада приготовленного на VIII научно-практическую конференцию „Information Systems In Management", которая состоится 21-22 ноября 2013 года.

Ключевые слова: *информационная безопасность, системы управления информационной безопасностью, политика информационной безопасности*